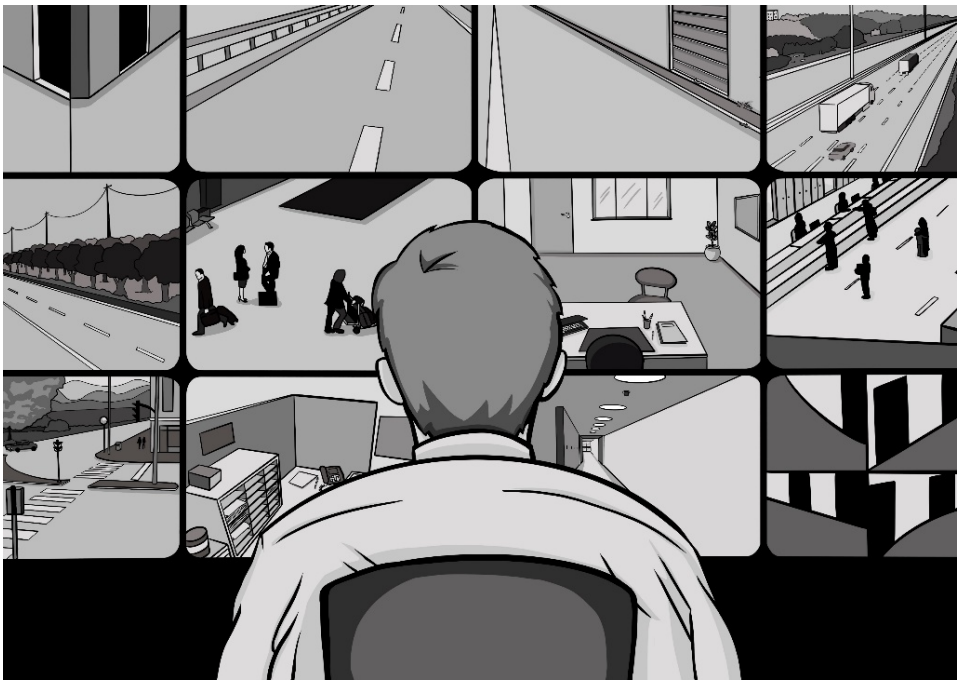
Essential Concepts and Principles for the Use of Video Evidence for Public Safety and Criminal Justice

By Martino Jerian, CEO and Founder, Amped Software



A set of general concepts and principles to support policymakers, law enforcement organizations, judges, and legal system stakeholders, in the proper use of images and videos for public safety and criminal justice purposes.

Foreword

Videos and photos permeate many aspects of our society. Different studies have shown that video evidence is one of the most important and powerful sources of information for investigators, analysts, and judges. Despite its importance, it is often not treated as rigorously as other forms of scientific evidence, such as DNA and fingerprints. Video is one of the main tools to understand the dynamics of an event and identify its perpetrators but working with it in the right way - and correctly interpreting it - is not as easy as it seems.

The purpose of this document is to outline some very important principles that all the stakeholders of a public safety organization and the criminal justice system should be aware of to get the best results during investigations, grant a fair and transparent trial, and minimize the risk of a miscarriage of justice through improper use of image and video evidence.
The principles we are outlining in this document should be already well-known and understood by forensic analysts and technicians. However, a large amount of video evidence is handled locally by first responders and investigators, who may lack the competency and technical foundations to work with such evidence and correctly deliver it to the legal system.
The incorrect handling of videos and images can have huge implications for our safety and security, from missing important details during police operations to following a wrong path during investigations, causing costly mistakes that could lead to crucial evidence being dismissed in court or condemning the wrong person.

Knowing and following these basic principles will lead to a more secure public environment, fair and correct trials, and a quicker, more efficient, and less costly justice system.

FOREWORD **2**

UNITED NATIONS UNIVERSAL DECLARATION OF HUMAN RIGHTS **7**

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION **8**

INTRODUCTION **9**

INSTITUTIONAL SECTION **11**

Main Issues and Risks Connected to Video Evidence **12**

1. Video evidence seems easy, but it's actually easy to get it wrong 12
2. Proprietary video formats complicate investigations and introduce cybersecurity risks 13
3. Image quality is often low: it must be enhanced in the right way 14
4. We can't always trust video evidence: deepfakes, manipulation, and misattribution 15
5. Judges and juries are easy to mislead on technical topics 15
6. Impact of Artificial Intelligence 16
7. Privacy and Cybersecurity 16

Working Correctly With Video Evidence: 4 Essential Concepts **17**

1. Awareness and education 17
2. Originality and acquisition 17
3. Authentication and verification 17
4. Correct and transparent processing 17

Advantages of Working Properly With Video Evidence **18**

1. Improved safety and security 18
2. Better justice 18
3. Improved efficiency 18

TECHNICAL SECTION **19**

Part A: Technical Preparation **20**

1. Have a specific question and purpose for the media 20
2. Have the right skills, the right training, and the right tools 20

Part B: Acquisition, Authentication, and Verification **21**

3. Acquire the original files 21
4. Accurately convert and display the files 22
5. Verify the integrity and authenticity of the files 23

Part C: Correct and Transparent Processing **24**

6. Focus on the parts of interest 24

7. Identify the image issues and their cause 25

8. Process files with a scientific workflow 26

9. Use algorithms appropriate for forensics 27

10. Apply the algorithms in the right order 28

11. Choose the right parameters 29

12. Follow the guidelines 30

Part D: Analysis and Presentation **31**

13. Quantify, whenever possible 31

14. Employ bias limitation techniques 32

15. Write an objective and reproducible report 33

16. Present and explain your work in a simple, correct, and effective manner 34

CONCLUSIONS **35**

REFERENCES **37**

About the author **37**

About Amped Software **37**

Contacts **37**

United Nations Universal Declaration of Human Rights

Article 3
Everyone has the right to life, liberty and security of person.

Article 6
Everyone has the right to recognition everywhere as a person before the law.

Article 7
All are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination.

Article 9
No one shall be subjected to arbitrary arrest, detention or exile.

Article 10
Everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations and of any criminal charge against him.

Article 11
1. Everyone charged with a penal offence has the right to be presumed innocent until proved guilty according to law in a public trial at which he has had all the guarantees necessary for his defence.
2. No one shall be held guilty of any penal offence on account of any act or omission which did not constitute a penal offence, under national or international law, at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the penal offence was committed.

Article 12
No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 28
Everyone is entitled to a social and international order in which the rights and freedoms set forth in this Declaration can be fully realised.

Charter of Fundamental Rights of the European Union

Article 6
Right to liberty and security
"Everyone has the right to liberty and security of person".

Article 8
Protection of personal data
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Article 13
Freedom of the arts and sciences
The arts and scientific research shall be free of constraint. Academic freedom shall be respected.

Article 20
Equality before the law
"Everyone is equal before the law".

Article 21
Non-discrimination
1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.

Article 47
Right to an effective remedy and to a fair trial
Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.

Introduction

Given the ubiquity of video surveillance systems, the popularity of smartphones, and the widespread use of social networks, images and videos are nowadays some of the major sources of evidence during criminal investigations[1][2]. It's very rare to investigate a crime that doesn't involve some form of digital photo or video. No other kind of evidence can so often answer all the questions of the so-called "5WH investigative method"[3]: *who*, *where*, *what*, *when*, *why*, and *how*.

The main issue, from a public safety and justice perspective, is that this kind of evidence is often not handled with the same care and rigor dedicated to other types of evidence. Video evidence seems easy to interpret, but it's actually easy to get it wrong. Without the proper workflow, competencies, and tools, there's a risk of either driving investigations in the wrong direction or having evidence that does not stand the scrutiny of the courtroom.

Since we don't know what we don't know, the first step to addressing a problem is to make people aware that they have one. For this purpose, this document has been divided into two sections: the **first section is specifically aimed at policymakers and all the stakeholders of the public safety and justice system**, to make them aware of some very high-level **concepts** that they should take into account when dealing with cases involving image and video evidence; the **second section**, **is aimed at practitioners** of the image and video forensics discipline and contains the actual **principles**. With the term *practitioner,* we mean any individual, with different roles, responsibilities, and competencies, who works with image and video evidence. Most of the principles should be already well known by experts and analysts (either from law enforcement, other government agencies, or the private sector), while they may be newer to first responders, investigators, and officers. The principles are indeed especially important for these less specialized roles: while they usually have many other technical and non-technical duties, they are those who deal with video evidence on the front line.

A final word for what regards the terminology: the field we are writing about is called in a variety of ways, with close but slightly different nuances: *forensic image/video analysis*, *image/video forensics*, *multimedia forensics*, *digital multimedia evidence* (DME), or simply *video evidence*. In literature, the most widely used definition is: "*Forensic video analysis is the scientific examination, comparison, and/or evaluation of video in legal matters*."[4] In the following, we will use the terms *image* or *video* indifferently, as normally a video is considered a sequence of images, possibly with an additional audio component, or metadata such as timestamps or GPS locations.

The concepts and principles that follow will be described by an easy-to-understand sentence and a more detailed explanation that gives some introduction to the topic and issues.

[1] Ashby, M.P.J. The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis. Eur J Crim Policy Res 23, 441–459 (2017). https://doi.org/10.1007/s10610-017-9341-6

[2] https://pure.southwales.ac.uk/ws/portalfiles/portal/3994343/HIFS_Project_Research_Insight_3._The_Use_of_CCTV_during_Homicide_Investigations_Contributions_Challenges_and_Risks_April_2020_.pdf

[3] Stelfox, Peter. (2013). Criminal Investigation: An Introduction to Principles and Practice. 10.4324/9781315880730.

[4] https://www.swgde.org/glossary

INSTITUTIONAL SECTION

FOR POLICYMAKERS
AND STAKEHOLDERS
OF PUBLIC SAFETY ORGANIZATIONS
AND THE JUSTICE SYSTEM

Main Issues and Risks Connected to Video Evidence

1. Video evidence seems easy, but it's actually easy to get it wrong

Anybody can hit "Play" or download a photo on their PC and try to interpret it. Because of these very low entry barriers, those who have to deal with video evidence may not have the proper technical preparation or the right tools, without being aware of that.

The generation process of digital images is made of many steps, many of which are unknown to the average person. Most of these steps influence the way reality is represented in the video. Some examples follow; please notice these are very common issues, they are not the exception:

- The typical "black & white image" created by surveillance cameras in **"night-vision" mode** does not carry any information about the visual color of objects: a **checkered shirt typically looks perfectly uniform** in these grayscale images[5].

- Surveillance cameras' **lenses cause a distortion** in the image, so a recorded **subject may look way taller and thinner** than they actually are. Besides that, every measurement taken from a video will be wrong if the distortion is not taken into account[6].

- The conversion from analog cameras to digital video often has a **wrong aspect ratio** (that is, the proportion between the height and the width of the video). This can easily **turn an SUV into a limousine** in the generated video[7].

- Strong video compression may **remove details that were present** at the crime scene: this may result in a **scar disappearing from someone's face**. At the same time, compression may also introduce digital artifacts that could be mistakenly considered real details of the crime scene: compression can easily **add a mole on a suspect's face[8]**.

It is straightforward to understand that even a single one of the mentioned artifacts, if not understood and compensated for, can steer an investigation in the wrong direction, and even lead to the wrong person being arrested. Of course, these defects add together during the video generation process, so that the video evidence is often way farther from the reality of events than we may think.

[5] https://blog.ampedsoftware.com/2021/01/19/infrared-dont-trust-the-colors-of-most-cctv-footage-at-night/
[6] https://blog.ampedsoftware.com/2021/02/02/lens-distortion-cameras-may-change-the-shape-of-things/
[7] https://blog.ampedsoftware.com/2021/01/26/aspect-ratio-be-sure-your-image-is-not-stretched-in-either-direction/
[8] https://blog.ampedsoftware.com/2021/04/13/compression-artifacts-hiding-or-adding-details-to-the-scene/

2. Proprietary video formats complicate investigations and introduce cybersecurity risks

Most surveillance devices record videos in proprietary formats that will not play with standard software. Even the basic playback of such videos is a challenging task that often frustrates officers and practitioners. If videos are "converted" in the wrong way, the quality and reliability of the evidence could be severely impaired.

The vast majority of files coming from video surveillance systems are in a proprietary format. This means that usually, **they are not normal MP4 or AVI files** that can be played with standard software, such as Windows Media Player or VLC, but they need the player created by the system producer. Very often, these players are of low quality, have significant issues, and are completely inadequate for a forensic analysis of the video.

In order to perform video analysis, most of the times **proprietary files need to be converted**. This is another critical phase. A conversion done without the proper care can very easily introduce these issues[9]:

- **The loss of file integrity**, with a clear impact on the chain of custody that we must ensure for every kind of evidence. For example, an improper conversion will lead to work with data that is not the best evidence.
- **The loss of quality**: if the video is re-compressed as part of the conversion, this may cause a noticeable quality loss.
- **The loss of metadata and information** about the original encoding, such as timestamp and the kind of compression applied on different parts of the image; this information could have been used to evaluate the reliability of the visual information.

Furthermore, the search and use of proprietary players can cause many issues from the IT and cybersecurity points of view.

Poor handling of video evidence is usually more dangerous than poor handling of other kinds of forensic evidence. For example, when a biological sample is not preserved properly, DNA analysis may become impossible, thus leading to loss of potential evidence. If video is not handled properly, it will typically reach the court anyway, but it may easily **show an altered version of the events**. Furthermore, it is usually easier to implement a proper chain of custody for video evidence than for physical evidence.

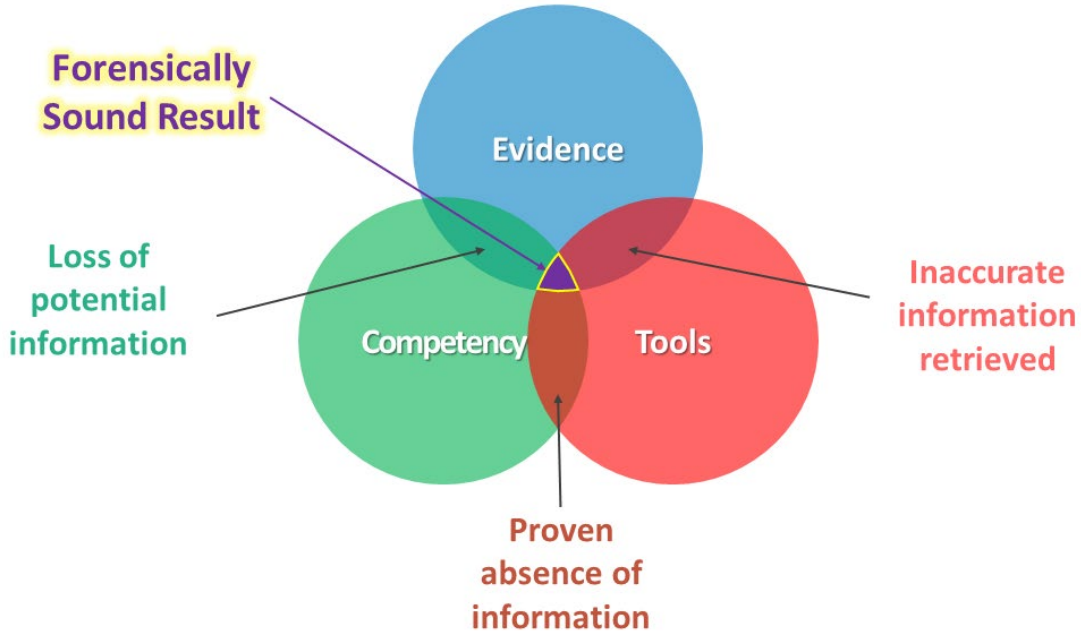
For example, there was a case where an officer was charged with **throwing an arrested subject against a wall** on the sole basis of surveillance recording; it later emerged that, due to the wrong conversion, the **playback speed was changed** for that fraction of the event, and the officer was acting respectfully.

[9] https://blog.ampedsoftware.com/2021/03/16/proprietary-cctv-dvr-players-often-not-showing-the-original-pixels/

3. Image quality is often low: it must be enhanced in the right way

Video evidence often doesn't have sufficient quality to obtain the needed information, for example, to identify a person or a vehicle. However, using the right tools and techniques, if there are the right technical conditions, it can be enhanced with excellent results.

It is fundamental to understand that a good result in forensics analysis is always the combination of three elements, none of which is optional: **evidence, competency, and tools**. This concept is better explained by this diagram:



The processing must be done in a **rigorous** way, using methodologies applicable to the forensic settings and **scientifically validated**; otherwise, the evidence could be disqualified during the trial. Forensic video enhancement should **never create new information**, it should rather make the existing information better available.

According to research carried out by Amped Software through a user survey in 2021[10], video enhancement can produce useful results in almost 60% of cases.

[10] https://blog.ampedsoftware.com/2022/02/15/a-survey-on-video-evidence-the-highlights-from-the-amped-user-days-2021/

4. We can't always trust video evidence: deepfakes, manipulation, and misattribution

We grew up in a world where seeing was believing, but the last two decades witnessed a flourishing of manipulation techniques that create visually credible forgeries. When considering whether an image should be admitted as evidence, it is important to ask ourselves: "Is it authentic?". Authenticity means that the image is an accurate representation of what it purports to be.

Authenticating images and videos is becoming of utmost importance. Lately, **deepfakes** (that are manipulated images created using artificial intelligence techniques) are everywhere in the news. They can be weaponized to ruin the **reputation of a politician**, creating a video where they say things they never said, or for **sexual harassment**, e.g. by swapping someone's face into the face of a pornographic actor. They've been used in the **Russian-Ukrainian war** in 2022 to impersonate the Ukrainian leader and make him order soldiers to surrender[11].

In actual cases, however, it is yet more common to encounter **"standard" fakes**, created using photo editing software. They can be used to **create a false alibi,** perpetrate **insurance frauds**, etc.
It's not even needed to modify an image to use it in a malicious way: it may be sufficient to reuse a photo done at another time or staging an event and claiming it happened. All this is much easier to do than a deepfake or even a manipulation with a software like Photoshop.

For these reasons, it is important to consider **whether an image should be trusted** before admitting it as a source of evidence.

5. Judges and juries are easy to mislead on technical topics

The challenges of video evidence should not be underestimated: whenever appropriate, expert witnesses should be called. However, it's often difficult for judges, juries, and the public to evaluate the technical ability and reliability of the various sides' expert witnesses. Therefore, it is important to consider their contribution with the maximum possible objectivity.

As explained in the above points, image and video forensics is a **complex discipline, full of pitfalls**. It is unreasonable to assume that judges and juries have the technical expertise to understand all the details behind an analysis. However, they should understand that video forensics must be treated with the same cautiousness as every other forensic discipline.
"Common sense" should not be admitted as a valid criterion, as it would not be admitted when discussing a DNA, fingerprint, or calligraphic comparison.

Presentation of video evidence is an important issue. When video evidence is to be presented, suitable equipment should be available, and any "on-the-fly" adjustment to prepare evidence should be avoided, as it often negatively impacts the repeatability of the presented result. For example, even a simple "zoom in" on the presented footage should only be done by a qualified professional.

[11] https://www.youtube.com/watch?v=X17yrEV5sl4

6. Impact of Artificial Intelligence

AI processing on video evidence should be handled with extreme caution. Using AI to enhance images often produces new images whose generation process cannot be explained by an expert.

Artificial Intelligence is affecting many aspects of our lives, and it is certainly an important driver for development. Recent AI technologies, such as deep neural networks, deliver outstanding performance when used to enhance or analyze images and videos. However, despite relevant efforts from the research community, it is still believed that **results obtained with deep learning are poorly explainable**. In other words, deep neural networks tend to act like efficient and effective **black boxes**, meaning that even experts in the field (or potentially software developers) can not explain the logic behind the final result.

If we want to adhere to the undisputed principle that any image produced as part of a **forensic analysis should be repeatable and explainable**, then AI should not be used for forensic video enhancement tasks to provide the AI processed image as evidence (e.g., facial super-resolution, improving a license plate's image, noise removal, etc.)[12].

AI could be considered, instead, for video analysis (e.g., detect child abuse content, look for a suspect's face in a database of facial images, etc.). However, some important safeguards must be in place: the performance of the employed system should be known; the final decision should always be made by an expert; bias mitigation techniques should be used to avoid the expert being excessively influenced by the AI system.

The above concerns are motivated by historically agreed requirements for forensic methods and the fact that most video enhancement AI techniques are not explainable. Future policies could bring new sensitivity about requirements, as well as more explainable AI techniques.

7. Privacy and Cybersecurity

Working within the boundaries of privacy regulations is a very important aspect that should be taken into account even (and especially) by law enforcement. Since sensitive information is being treated, software and systems should be safe, as much as possible.

There is a natural tension between the need to acquire as much data as possible during investigations, their **forensic use, and privacy considerations**. Worldwide, there's growing adoption of stricter privacy frameworks that typically follow the steps of the European GDPR. With a few exceptions, working in, or for, the judicial system doesn't exempt us from such regulations.

Also, the cybersecurity aspect is very important. Forensics and investigation are by nature sensitive industries, where data and security must be taken very seriously. Software and systems should be safe so as to **avoid leaking sensitive information** or allowing cybersecurity attackers to alter them.

[12] https://blog.ampedsoftware.com/2021/10/05/can-ai-be-used-for-forensics-and-investigations/

Working Correctly with Video Evidence: 4 Essential Concepts

The above-mentioned issues could be solved. The overarching idea is that we need to create awareness and culture on this topic at 360 degrees. These issues should be solved both down and up the chain of command.

Once digested that video evidence should not be taken for granted, but should be handled scientifically and with care, we would need to create awareness programs for all the parts of the judicial system. It's not needed, nor recommended, that all police officers, attorneys, and judges would become forensics experts, but it's essential to create a cultural basis where everybody understands the importance and sensitivity of video.

What are the main concepts?

1. Awareness and education

Educating the users and the public on the pitfalls and complexities of video evidence. Expose people involved in the field to some form of short education program (a few hours) to open their eyes to the concepts that are currently unknown to most people.

2. Originality and acquisition

All the operators should understand the importance of a correct acquisition. Too often, we see surveillance video footage wrongly captured filming a screen with a smartphone. A proper acquisition should be followed by a rigorous chain of custody in order to guarantee access to the original evidence and disclosure of every action taken on it. This would grant the best possible quality and reduce the risk of the evidence being rejected in court.

3. Authentication and verification

Verifying the integrity of the file (is it original and unaltered?) and how much we can trust its content authenticity. Furthermore, this process should be able to verify that the acquisition has been carried out properly.

4. Correct and transparent processing

Adoption of clear guidelines for processing, using algorithms validated by the scientific community, and adopting a workflow that is correct, repeatable, and reproducible. There are several guidelines of

excellent quality available, such as those from ENFSI[13], SWGDE[14], OSAC[15], and the UK FSR[16]. They should be more widely followed and adopted.

Advantages of Working Properly with Video Evidence

Working correctly on image and video evidence, keeping in consideration the concepts mentioned in the previous section, and more specifically following the principles further explained in this document, has several advantages that can improve different aspects of our society.

1. Improved safety and security

Working correctly allows us to streamline the processing workflow instead of reinventing the wheel every time. While it's true that every case is different, the underlying issues and objectives of an investigation are often very similar: most of the time, the purpose of the analysis is to identify a person, a vehicle, or understanding the dynamics of an event.

Working correctly would allow us to solve more crimes, and thus **improve the safety and the security of our cities and countries**.

2. Better justice

Using original data, assessing their authenticity and integrity, and processing them in the right way, courts will be better able to assess and then apply the video evidence in their fact-finding role, thus lessening the risk of unjust outcomes. In this way we can **grant more fair trials and reduce judicial errors**.

3. Improved efficiency

Doing things the right way does not take more time, it actually involves a more efficient workflow. This means **less time** spent by human resources and **fewer issues** caused by mismanaged evidence.

[13] https://enfsi.eu/about-enfsi/structure/working-groups/documents-page/documents/best-practice-manuals/
[14] https://www.swgde.org/documents/published-complete-listing
[15] https://www.nist.gov/topics/organization-scientific-area-committees-forensic-science/osac-standards-and-guidelines
[16] https://www.gov.uk/government/publications/video-analysis-codes-of-practice-for-forensic-service-providers

TECHNICAL SECTION

FOR

PRACTITIONERS

WORKING

WITH VIDEO EVIDENCE

Part A: Technical Preparation

1. Have a specific question and purpose for the media

Do: *make sure questions are clearly defined before starting any job.*
Don't: *don't start analyzing a video without a clear purpose, and don't accept generic requests such as "look for interesting information" or "enhance the quality".*
Risks: *wasting time and possibly introducing bias in the video investigation.*

Analyzing an image or video is just a means to an end. It is necessary to know what we are looking for. It doesn't make sense to forensically "enhance" an image without a clear purpose. Most of the time, processing an image will deliver a less pleasant result globally but provide more clarity on the parts of the image where the relevant information is located. For example, if we enhance a license plate, we often lose quality in other parts of the image.
Generally, the two most common requests during video investigations are related to the identification (typically of a person or a vehicle) and the reconstruction and understanding of a sequence of events. Following this principle will drive the analysis in the right direction, waste less time, and have a better outcome. How can we answer a question if we don't know what we are looking for?

2. Have the right skills, the right training, and the right tools

Do: *video analysis should be taken seriously, like any other technical investigation, you should have the competencies and the tools adequate for the tasks being requested.*
Don't: *don't perform a task you are not prepared for, and if you don't have the option to refuse, clearly highlight the risks of doing the job.*
Risks: *causing an excessive waste of time, driving the investigation in the wrong direction, and potentially having evidence disqualified in court*

Video evidence seems easy to understand because it's something everybody can see, but underneath the surface, there are a lot of complex mathematical and technical concepts. In fact, image processing is ultimately a visualization of some mathematical operations.
People should have the right technical skills and receive the training and education needed for their roles (such as investigators, technicians, and analysts). Furthermore, many general-purpose tools, such as standard players or creative-oriented image editing software, lack the rigor and transparency needed for forensic applications, lack essential functions, or make things more complicated than they should be. They often needlessly expose the operator, and the evidence, to risks, using methodologies and tools inappropriate for forensics.

Part B: Acquisition, Authentication, and Verification

3. Acquire the original files

Do: *ensure to obtain the best possible evidence, which ideally means the original version of the footage.*
Don't: *don't analyze images and videos sent via email, social media, messenger apps, screenshots, or screen captures of a monitor, unless there is absolutely no other way to get better or more original files.*
Risks:
- not being able to recover crucial details that could have been obtained on an original;
- losing important metadata (such as timing and GPS information);
- introducing in the chain of custody unreliable evidence (and that can cause evidence to be rejected).

The analysis work should start from the original video files. This is easier said than done. Most of the video surveillance footage used during investigations comes from *CCTV* (from "closed-circuit television") connected to small low-cost appliances called *DVR*s (from "digital video recorders"). These systems have several export options for retrieving the footage. Most DVRs have a combination of proprietary formats as well as standard formats. The most common error that is carried out when retrieving CCTV is exporting the footage into a familiar, yet converted format, such as AVI, MOV, or MP4. It is essential to recover the original footage in whatever format it exists at creation. Furthermore, images and videos from mobile devices are often converted when shared with various applications or transferred to a PC.
If files are not acquired with the proper procedure, we face two significant issues:

a) From a forensic and judicial perspective, we **break the chain of custody**, which is essential for the acceptability of every kind of evidence;
b) We may cause a **loss of information and/or quality** and a **loss of original metadata** that can contain fundamental information for the case (such as camera names, timing, GPS information, settings, compression type, and so on).

It must be said that it's not always possible to get the original: sometimes it may have been lost, damaged, or simply not available, especially when working on data coming from the cloud or social media. But even in this case, care should be taken to get the file closest to the original or having the best quality, and when needed, provide a justification for why the original is not being used.
The worst case, which happens way more times than it should, is to receive a CCTV video obtained by filming the monitor of a surveillance system with a mobile phone. This is not "the evidence": that is *a video of the evidence*. It's like doing a ballistic analysis on a photo of a bullet instead of the bullet itself. The original digital file is the evidence, not just its visual content. There's so much useful information that is not visible to the naked eye.

4. Accurately convert and display the files

Do: *convert and display the files preserving the original data as much as possible and preventing further quality loss.*
Don't: *don't blindly trust proprietary CCTV/DVR players and their exported files. Don't screen capture a video from the system, or even worse, film a video surveillance monitor with a mobile phone, unless that is the very last resort.*
Risks:
- not being able to recover crucial details that could have been obtained on an original;
- losing important metadata (such as timing and GPS information);
- introducing in the chain of custody unreliable evidence (and that can cause evidence to be rejected).

As explained above, when speaking about videos coming from CCTV, most of the time the original files are in a proprietary format (they are not simple AVI, MOV, or MP4 files). These files need to be played either in a special software given by the system producer or converted to make them compatible with other players or processing software.
There are hundreds, if not thousands, of different formats and players on the market. Often these systems are not adequate for a forensic analysis of the video, and when they supply export facilities, the conversion may cause quality loss and other issues.
An accurate conversion and display of the files can be obtained by those with good knowledge of the video forensic field or by utilizing specialized forensic software which takes care of accurately processing the files. Unfortunately, there are cases where the video can not be exported correctly or at all, so the only possibility is to use another software to capture what's happening on the screen while playing the video. This should be considered the last resort, as it's very error-prone: the result depends on the playback accuracy of the player, the capability of the capturing system to avoid duplicated or missing frames, and compression settings. In any case, the result will be a file dramatically different from the original, even if the visual part could be quite close if done properly.

5. Verify the integrity and authenticity of the files

Do: *copy files with a forensic procedure (like comparing hash codes), be wary of possible clues of the file not being an original (for example a video from a CCTV in AVI format often won't be an original) and consider possible signs of manipulations.*
Don't: *don't copy files without verifying the source and destination of the copy, and don't blindly trust their content.*
Risks:

- *starting the analysis on files that have not been copied or acquired in the best way, causing the quality and integrity issues highlighted in the previous points;*
- *trusting unreliable evidence.*

At this point, we have some files we are able to display and analyze. But can we trust them?
We need to perform two different kinds of analysis: *integrity verification* and *authentication*[17].

Integrity verification is *the process of confirming that the data presented is complete and unaltered since the time of acquisition*. It can usually be performed quite easily by comparing a secure hash code (a unique file identifier) of the original evidence with the working copy.
Authentication is *the process of substantiating that the data is an accurate representation of what it purports to be*.
What's the difference between integrity and authenticity? Let's explain it with an analogy. A real passport is an original and authentic document. If we make it a photocopy, that's no longer the original, but as long as it represents the actual data of a real person, it's authentic. On the other hand, a counterfeit passport of a person who doesn't exist may be the "original," - physically speaking - but it's not authentic.
A manipulated photo, where a subject has been removed from the image, won't be an original, nor an authentic image. On the other hand, if we stage an event and take a picture of it in order to pretend it happened, we could have an original photo that is not authentic.
A very common, and often difficult, case is to authenticate images coming from social media. Social networks usually recompress images and videos and remove most metadata. We can easily verify that these files are not the original, but traces of manipulation are usually covered when the data is recompressed aggressively or multiple times, as often happens in these cases.

In some cases, the core of the analysis can be focused on determining the integrity and authenticity of a video or image. However, this is a fundamental step that must be done, even at a very basic level, in all cases related to images and videos. It could be as simple as asking ourselves if there's any reason not to believe that the video is the original and that we can trust its content.

For example, if we acquire a video coming from a CCTV in a standard format and not in a proprietary format, very often it hasn't been acquired in the way described in principle number 3. We should then ask ourselves: "why is it so?" and "can we still get the original?". On the other hand, if an image has been given by a party involved in an investigation, more care should be given to assessing how much we can trust it.

[17] https://www.swgde.org/glossary

Part C: Correct and Transparent Processing

6. Focus on the parts of interest

Do: *acquire enough data at first, then identify the parts of interest for the investigation and focus on those.*
Don't: *don't analyze and process the entire footage available if it doesn't contain useful information unless you've been explicitly asked to do so.*
Risks:

- *working on the entire footage, even when it doesn't contain useful information, may cause a huge waste of time and resources;*
- *suboptimal processing and analysis on parts of interest.*

Most of the time, we need to find a needle in a haystack. We may collect hours of videos from multiple cameras, looking for a subject or an event that lasts only a few frames. This process may be fast and easy, long and complicated, or everything in between.
It's hard for human operators to focus their attention on videos or images for hours, looking for some small details. Specialized software exists to sift through all this data. While it can be of great help, this can miss important events or details (especially when the quality is low) or give a lot of false alarms. Ultimately it is our responsibility to validate and know how much to trust the result of these semi-automated systems and be sure all the critical information has been identified.
Once the parts of interest are identified, it's important to focus on those and find the optimal processing for them. The optimal way of processing the entire video may not be the best one for the specific parts of interest.

7. Identify the image issues and their cause

Do: *analyze and understand the quality issues and technical problems affecting the images before doing anything.*
Don't: *don't process images without a clear understanding of the problems to be solved.*
Risks:

- *a suboptimal improvement or even a worse quality than the original, possibly introducing unwanted artifacts;*
- *the lack of a proper justification for the processing could cause the evidence to be rejected in court.*

Often the video won't be able to answer all of our questions straight away. Identifying the issues and understanding if and how we can cope with them is one of the most complicated but important parts of the analysis. Most of the time, these relate to image quality, but not exclusively.

This is a non-exhaustive list of typical issues found in digital images and videos[18].

- **Low spatial resolution** on the details of interest: not enough pixels on an area of interest.
- **Low temporal resolution**: low frame rate can cause short events not to be represented in the video.
- Image and video **compression,** which causes a loss of detail and artifacts.
- **Blur**: where an image appears out of focus or smeared with fast-moving subjects.
- **Noise**: random or periodic variations of pixel values, often visible as "grain" in low-light images.
- Strong **perspective distortion** makes it difficult to view details from a strong angle.
- **Lens distortion**: makes straight lines appear as curved.
- **Brightness**, **contrast**, and **color** issues: cause unreliable colors, images that are too dark or too bright, or low visibility of details.
- **Aspect ratio** distortion: the ratio between the width and height of the image is wrong, making subjects appear squished and thus with the wrong proportions.
- **Interlacing**: a heritage of analog systems which causes a combing effect on moving scenes.
- **Timing** issues: wrong playback speed or unreliable timing information.
- Others: missing or duplicated frames, rolling shutter artifacts, decoding errors, and so on.

In a typical case, several of these issues are present in one form or another, so it's important to understand which ones can and should be corrected. In fact, there are issues that under certain conditions can be properly corrected (such as a dark or blurred video), and others that can't (such as converting an infrared video to visible light colors).

18 https://blog.ampedsoftware.com/2022/09/13/the-image-generation-model-cheat-sheet-included

8. Process files with a scientific workflow

Do: *define, document, and use a correct, repeatable, and reproducible workflow for all your cases.*
Don't: *don't process files without a systematic approach.*
Risks: *not being able to explain what you did and why, or even worse, not being able to replicate the same analysis again.*

Once we understand the issues affecting the image and the purpose of the analysis, we can proceed to work on the files. Image enhancement is an important part of the processing, though not the only one, and it's essential to remember that it's just a means to an end. We care more about getting useful and actionable information from a video than about having a visually pleasant image.
When we process files, we are handling evidence, so the workflow must follow a scientifically valid methodology that follows these principles[19]:

a) **Accuracy**: the processes should be as much as possible accurate and free from errors, and if possible, the error should be quantifiable. Methods should be based on scientific research as much as possible so that the tools and techniques are free (again, as much as possible) from bias and help limit the human bias by the operator.
b) **Repeatability**: we should be able to repeat the analysis at any time and be able to get the same results. It is a big issue if every time you get a different result.
c) **Reproducibility**: if we are the only ones able to get a specific result, then something's wrong. Following the documented procedure, a properly qualified third party should be able to reproduce the results obtained from the analysis at any time.

One of the most common questions is: "*How can I justify to the court the fact that I processed an image used as evidence?*" The reply is actually very simple: by understanding how defects are introduced and correcting them, we can obtain *a more natural representation of the scene* (or of some subjects or objects of interest) than the original images.

A very straightforward example is the lens distortion introduced by wide-angle lenses: straight walls appear curved in the image because of the features of the camera optics. **Since the actual walls are straight and not curved, the distortion correction allows producing an image that is a more reliable representation of the real scene.**

[19] https://blog.ampedsoftware.com/2021/10/05/can-ai-be-used-for-forensics-and-investigations/

9. Use algorithms appropriate for forensics

Do: *use only methodologies and tools which could be acceptable in a judicial context: they should be explainable by a competent practitioner, validated, deterministic, and don't introduce data external from that case that can bias the results.*
Don't: *don't use any algorithms, tools, or methodologies that don't satisfy the above requirements, no matter how promising the possible results are. For example, image enhancement algorithms based on Artificial Intelligence (AI) are usually not appropriate for evidentiary purposes.*
Risks:

- *driving the investigations on the wrong path;*
- *relying too much on results that seem clear but are not as reliable as expected;*
- *errors and biases in the results;*
- *having evidence rejected in court, because of the use of an unreliable methodology.*

The methodologies and algorithms that we use for forensics, should follow the principles of accuracy, repeatability, and reproducibility presented above. Otherwise, how can any forensic process be respected in practice? Practitioners should rely on algorithms with the following features:

a) **Explainable**: the algorithms should be understandable and explainable by a competent practitioner. Given the critical context in which work is done, it is necessary to understand the general workings of the algorithms in order to go over the possible scenario limitations of a "black-box testing" approach used to evaluate their accuracy and better guarantee reproducibility.

b) **Validated**: if possible, the algorithms should have been accepted by the scientific community. For example, many techniques have been published in a scientific journal after a peer review or in an academic book. If such a reference is unavailable, a detailed explanation of their functioning, allowing independent validation, may be acceptable.

c) **Deterministic**: in order to guarantee repeatability and reproducibility, the used algorithms shouldn't have random components. Some algorithms need a random number within their computational process; in this case, a possible workaround is to fix or document the random number generator seed, in order to get the same result every time the practitioner runs an analysis.

d) **No external data**: the output should be based only on a combination of the input data and the algorithm, with no data external to the case which could influence the processing. Notice that this is very important both at the algorithmic level and at the human level in the subsequent analysis.

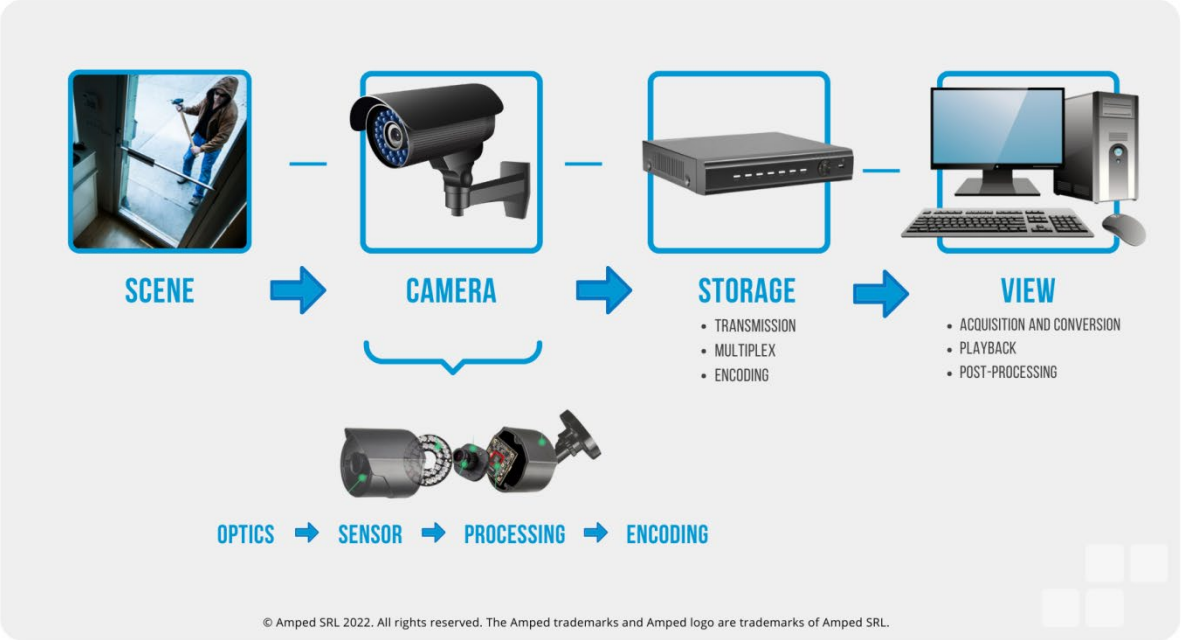
In general, following these points should allow working in a forensically sound manner. If some of the requirements are not respected, the admissibility of the processing may be in doubt. For example, there's currently a discussion about the applicability of algorithms based on Artificial Intelligence (AI) for certain forensics applications. In fact, AI techniques pose several challenges for what regards the explainability and the bias introduced by the data used to train the network.

10. Apply the algorithms in the right order

Do: *identify the defects that need to be corrected, understand the order in which they are introduced, and correct them in the reverse order.*
Don't: *don't apply the corrections in the wrong order and don't over-process, that is, don't correct defects when they're not impacting the requested analysis.*
Risks: *depending on the issues and the used algorithms, the process could be formally incorrect or cause more harm than good to the image. Issues that could be easily solved by applying the correction in the right order, could be impossible without following this rule.*

When processing files, there are usually multiple issues to correct, and they must be corrected in the right order. In order to do so, we need to understand the **image generation model**[20].

The image generation model represents a conceptual understanding of how the light from a scene in the physical world is captured by the camera, converted into an image, and, in the case of a digital image (or video), ultimately saved a sequence of zeros and ones.



In each step of the process, there are technical limitations that introduce some differences between what would be an ideal view of the real world and the actual depiction that we get out of the imaging process.

The footage we are working with is thus the product of a long acquisition and processing chain, which usually introduces several artifacts. The most reasonable way to compensate for these artifacts is in **reverse order**.

[20] https://blog.ampedsoftware.com/2022/09/13/the-image-generation-model-cheat-sheet-included/

Many different defects are introduced throughout the steps of the image generation model. Understanding the actual model for a specific case and which defect is introduced at each stage is key to enhancing the image in a scientific manner.

11. Choose the right parameters

Do: *choose the most logical and best-performing parameter values after appropriate inspection.*
Don't: *don't use wrong or imprecise settings.*
Risks: *using the right algorithms with the wrong parameters can either cause to have less than optimal results or even a result that is much worse than the original.*

Simply using the right algorithms in the right order is not enough. The result of an algorithm changes dramatically depending on the parameters used. You need to carefully choose the correct settings of the used algorithm, which may be unique to the image, in order to have the right output. If you apply a lens distortion correction or deblurring with a parameter that doesn't reflect the characteristics of the actual defect, you will likely get an image that is much worse than the original.

It is usually recommended to practice and experiment algorithms and tools on reference data with known ground truth, in order to understand how different parameters impact the final result in a controlled environment.

12. Follow the guidelines

Do: *use internationally accepted guidelines or organization-specific standard operating procedures.*
Don't: *don't reinvent the wheel. While every case may be a bit different, most of them can be reconducted to some pretty standard situations and thus should be tackled consistently.*
Risks:

- *not following what the wider community generally defined as a proper methodology;*
- *spending more time researching and testing the right strategy;*
- *tackling similar cases (or the same case by different practitioners) in different ways, thus raising doubts on the proper way to work;*
- *making more complicated and unreliable the work done by the opposing side's experts in court.*

While the principles of this document give a high-level overview of the most important topics when working with video evidence, there are several guidelines available at national and international levels that should be more widely followed and adopted. Some examples of guidelines, as already mentioned above, are those from ENFSI[21], SWGDE[22], OSAC[23], and the UK FSR[24]. Different guidelines provide a different amount of detail on specific topics, depending on their intended audience, but they are usually a great starting point for many fields since they are defined and promoted by the forensic, scientific, or legal communities.

Unfortunately, often they are not well known or adopted, which can lead practitioners to slow their processes down while trying to reinvent the wheel. From these guidelines, it is often appropriate to write organization-specific standard operating procedures (SOPs) that allow all members to produce and follow the same methodologies.

[21] https://enfsi.eu/about-enfsi/structure/working-groups/documents-page/documents/best-practice-manuals/
[22] https://www.swgde.org/documents/published-complete-listing
[23] https://www.nist.gov/topics/organization-scientific-area-committees-forensic-science/osac-standards-and-guidelines
[24] https://www.gov.uk/government/publications/video-analysis-codes-of-practice-for-forensic-service-providers

Part D: Analysis and Presentation

13. Quantify, whenever possible

Do: *try to measure and quantify the outcome of the analysis together with an error rate or a confidence interval, when it's possible and when it makes sense.*
Don't: *don't just "describe" something qualitatively.*
Risks: *not quantifying something objectively measurable opens the side to different interpretations, could be more error-prone, and may raise doubts in court.*

When working on images and videos, it is tempting to describe what is seen rather than measure it objectively. But due to several technical and human factors, it's often hard to objectively quantify and estimate something unless it is measured. Many popular optical illusions show how easily our senses can be fooled. One typical example is the wrong perception of sizes and distances because of the perspective.

When possible, it's better to measure something and provide **an error or a confidence interval** related to it. For example, rather than saying that two images look similar, we should document what's their difference mathematically with well-known descriptors (such as *SAD*, *SSIM*, or *MSE*). Various issues in the color and light of an image can be identified by looking at the image histogram and properly corrected. The height of subjects and speed of vehicles can be estimated numerically rather than qualitatively (as it's done with reverse projection).
While this is not always possible, and qualitative estimations may sometimes be needed, their subjective nature makes their strength and defensibility weaker than numerical methods.

14. Employ bias limitation techniques

Do: *ensure you are given only the information that is strictly needed for the analysis; prevent others from sharing details that could bias your work.*
Don't: *don't ask others what their results are before doing your analysis.*
Risks: *working on a case receiving too much information, can very easily influence the practitioner, introducing a bias that can drive the analysis into a wrong, or less accurate, outcome.*

Human factors determine a critical part of video evidence analysis. One of the most pressing issues is to limit human bias during the interpretation. Again, even just being aware of the issue is a good start, though it's not enough to solve it.

As a starting point, it is very important for practitioners to protect themselves from bias, agreeing to receive **only the strictly necessary technical information** to perform their job, and possibly refusing to receive any other information. It is very easy to get "too involved" in a case and instinctively seek confirmation for our beliefs and opinions. This can and often does happen because we are humans. Even without any malicious or explicit intent, our mind is used to exploit biases as a shortcut to difficult and complex situations.

A typical case is asking a colleague to verify a license plate, providing them with the sequence of characters we expect to identify. Especially when the intelligibility is low, it is very easy to be swayed to see what we expect to see. This is called **confirmation bias**.

License plates are just the tip of the iceberg: for example, facial comparison is an even subtler field. When enhancing a person's face, different processing may easily lead to a significantly different facial appearance. Therefore, it is fundamental that the practitioner who processes the video refrains from looking at the suspect's face beforehand, otherwise, they may tend to unconsciously "tune" the enhancement to make it a match (or vice versa, of course).

Furthermore, practitioners should be aware of the possible **bias induced by the system** over the human user and take the proper steps to mitigate it. If the practitioner receives a strong match by an automatic system (based either on AI or more "traditional" techniques) for a possible identification, they will likely be unconsciously biased towards a positive match. Perhaps the correct face has been mistakenly discarded by the system, and thus the examiner ignores it. In this regard, it's important to educate the practitioner on the limits of technology, how it can condition the operator's opinion doing the analysis, and adopt bias mitigation techniques, such as linear sequential unmasking and its evolutions[25].

[25] Dror IE, Kukucka J. Linear Sequential Unmasking-*Expanded* (LSU-*E*): A general approach for improving decision making as well as minimizing noise and bias. Forensic Sci Int Synerg. 2021 Aug 13;3:100161. doi: 10.1016/j.fsisyn.2021.100161. PMID: 34466797; PMCID: PMC8385162.

15. Write an objective and reproducible report

Do: *reply to all and only the questions being asked, stick to the facts, and don't go out of your areas of expertise. Request the help of a subject matter expert for topics outside of your competencies.*
Don't: *don't give information that hasn't been requested, personal opinions, or comments.*
Risks: *wrong results, a scientifically unreliable report, and exposing you in court to questions outside of your knowledge domain, possibly invalidating the work done.*

The output of your job should usually be some image or video files, a report, and maybe a presentation to deliver in court.
While doing so, it's important to **stay in your lane**; this means three different things:

1) **Reply to the questions being asked**. If you see other things of interest, you may need to inform the requestor, but without a complete picture of the case, you should generally stick to what you have been asked to do.
2) **Stick to the facts.** You should show the data and what you have been asked for, without expressing your personal views or opinions unless asked for and, in that case, be sure it's within your role (it may differ, in some countries, whether such role is that of a "technician" or an "analyst" or an "expert witness")
3) **Stay in your area of expertise.** If you are an image or video expert, it doesn't mean that you are also an expert on the content of the images. You should not perform face or car comparisons unless you also have that expertise. On this point, different jurisdictions have stricter or looser rules, but in general, it's better to seek the help of a subject matter expert in things that are out of your core competencies.

The report should be detailed enough to allow a third-party (with the right competency and tools) to review it and be able to reproduce the analysis independently. In fact, they should be able to process the original data following the process described in your report and obtain compatible results.

16. Present and explain your work in a simple, correct, and effective manner

Do: *objectively present the facts, and try to strike the right balance between an understandable explanation of your work in laymen's terms and technical correctness.*
Don't: *don't go too much into technical details, unless asked, or oversimplify the explanation to the point of saying something not correct that can be attacked.*
Risks: *not presenting effectively the work done, in a boring, or too complicated way can make it misunderstood thus limiting its usefulness or even harming your case. Conversely, oversimplifying it can expose you to attacks during cross-examination.*

Having done a technically excellent job is of little value if you are not able to **present it in the right way**. Judges, attorneys, prosecutors, juries, and the public usually have little scientific and technical knowledge. Yet, you should be able to explain things correctly and in simple and understandable terms.

It's often difficult for the above-mentioned stakeholders of the judicial system to **evaluate the technical ability and reliability** of the various sides' expert witnesses. Let's say that one side does a correct and very cautious analysis. The other side is less careful with respect to the various forensic procedures but gives a much stronger speech, maybe with an opposite outcome of the analysis. Often this is enough to cast doubts on the previous analysis, even if that was the correct one. Without a minimum of scientific and technical education and awareness, this is a very difficult issue to overcome.

Often, the **ability to communicate** is much more impacting than the actual correctness of the analysis.

At the presentation stage, there may also be other issues to consider. One important topic is to have the **right equipment**. This depends on the jurisdiction, but it's important to be aware of the means at your disposal when showing images and videos in court: are there some monitors, a TV screen, or a projector available? Do you need to use your laptop and pass it over? Or only printed images are acceptable? The effectiveness of the presentation relies on how well you are able to adapt to the limitations of the given environment.

Finally, it may be important, when applicable and required, to **redact sensitive parts of videos** and images, for example, faces or other personal information of people who appears in the footage.

Conclusions

The first objective of these concepts and principles is to raise awareness about the sensitivity of image and video evidence and give some indication on how to process them in a scientifically correct manner. These principles should be further developed, either independently or by adopting already existing internationally accepted guidelines. Only in this way, we can grant our countries better security, and better justice, and at the same time reduce costs for human resources and issues caused by mismanaged evidence. There are only advantages to working on video evidence in the right way. Only one major thing is needed: a change of mindset. **Video evidence is not "just a video", it's "evidence" and should be treated as such**.

References

About the author

Martino Jerian is the CEO and Founder of Amped Software. He graduated in Electronic Engineering at the University of Trieste (Italy) in 2005 (summa cum laude) with a dissertation on forensic image processing. He has an extensive software engineering experience, having designed and started the development of Amped Software products. In the framework of his career, he was appointed as a contract Professor at Tor Vergata University, as well as at Link Campus University in Rome, where he gave lectures related to investigations, forensics, and intelligence. He is currently focusing on the improvement of the relationship between science and justice, specifically during forensic investigations. He strongly believes that proper education and training are required when it comes to image and video analysis, as these technologies are often taken for granted. Raising awareness and advocating on the main video evidence-related challenges, especially in relation to cybersecurity and AI, are becoming one of Martino Jerian's goals.

About Amped Software

Amped Software is a software house that develops software for the analysis and enhancement of images and videos. Applications include forensics, security, and investigations in over 100 countries worldwide. Founded in Trieste, Italy in 2008, with a subsidiary in Brooklyn, NY, the company supports more than 1400 organizations in the public safety and national security fields. Amped Software relies on a team composed of 35 people from 10 different countries with varied backgrounds, including former law enforcement officers, physicists, military personnel, and experts in image processing.

Contacts

Martino Jerian
CEO and Founder
Amped Software
martino.jerian@ampedsoftware.com